

Control Web Content for Better Security and Productivity

Web Filtering

A Web Filtering solution is designed to restrict or control the content a reader is authorized to access, delivered over the Internet via the Web browser. It may be used to improve security, prevent objectionable activities, and increase productive within an organization.

Intelligent and Effective Content Control

Web-based threats such as Phishing, drive-by Malware sites, and Botnets are more sophisticated and scrutinized than ever, and as well as increasingly difficult to control due to the rise of mobility in the workplace, even more difficult for you to control. The Web has become the preferred medium of choice for hackers and thieves looking for new ways to disrupt services, steal information, and perform malicious activities for financial gain. In addition, employees who visit websites containing objectionable content can expose your organization to civil or criminal liability.

FortiOS Web Filtering solution utilizes three main components of the web filtering function: the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service. These functions integrate with each other to provide maximum control over what the Internet user can view as well as protection to the network from many Internet content threats. Web Content Filtering blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic by independent real-world tests.

Key Features & Benefits

Cloud based Rating Database	Real-time website category rating provides accurate content control
Wide choice of web filtering technologies	Various web filtering technology options are available to provide each organization the most suitable implementation.
Integrated with other security and networking functions	Allows organizations to simplified networks and reduce TCO.

Highlights

- Comprehensive and advanced Web Filtering features Safe Search and user override options
- FortiGuard Web Filtering Services with superior coverage of over 250 million rated websites
- Integration with other FortiOS components, such as User Identification for flexible and secured implementation.



FEATURES

Cloud-Based Rating System

Fortinet is a pioneer in cloud-based rating systems for web filtering. FortiOS provides an innovative approach to HTTP and HTTPS web filtering technology by combining the advantages of a cloud-based service offering with layered response caching. The multiple FortiGuard data centers around the world hold the entire categorized URL database and receive rating requests from FortiGate units triggered by browser-based URL requests. FortiGuard responds to these rating requests with the categories stored for specific URLs, the requesting FortiGate unit then uses its own local profile configuration to determine what action is appropriate to the category, such as: blocking, monitoring, allowing the page, displaying a warning, or requiring authentication to view the page.

Rating responses are also cached directly in FortiGate unit memory so that ratings for frequently used sites can be retrieved directly from the cache, reducing the number of requests to the FortiGuard network. Caching URLs in memory makes URL lookups almost instantaneous while only using a very small amount of system memory.

An appropriately licensed FortiManager appliance can be synchronized to the FortiGuard network and as such can be used in the same way to as the FortiGuard network for managed FortiGate devices. This can further reduce any latency associated with the round trip time for individual rating requests while at the same time ensuring complete database coverage. Consider the combination of a LAN attached FortiGate cluster and FortiManager combination with the potential to handle tens of thousands of requests per second.

Superior Coverage

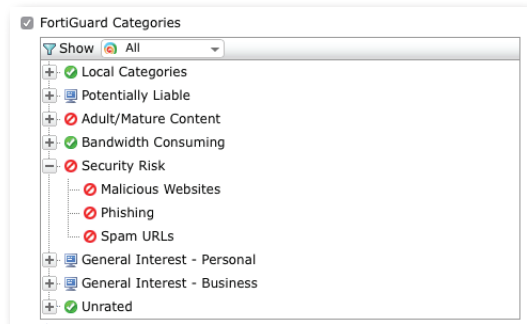
FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. This service currently rates more than 250 million sites covering billions of URLs with each site able to be rated in multiple categories. The FortiGuard database provides a truly international service with support for 70 languages.

Extensive and Flexible Categorization

Rated URLs are assigned into one of the 98 categories (including 20 user defined ones) which administrators can then easily manage and control. Administrators can configure and populate local categories or place specific URLs in existing categories should the FortiGuard rating not be in agreement with an organization's policies and practices.

Rating Override

At times, administrators may have to allow approved people to access what they need during periods when an exception to the normal rules is required, while still having enough control that the



organization's web usage policies are not compromised. FortiOS can provide such setup by using alternate profiles.

Protection against Malicious URLs

The malicious URL database contains all malicious URLs active in the last month and is organized as one of the categories.

With Fortinet Security Fabric, customers can further their protection by having the FortiSandbox add newly discovered URLs to a dynamic URL filter, thus blocking files from being downloaded again from that URL.

Inspection Modes

FortiOS web filtering can operate in three modes. Each mode has strengths and weaknesses and all three can be active at the same time on different traffic streams.

Proxy-based web filtering uses a proxy to assemble and analyze web content as it passes through the FortiGate unit. If a page is blocked the proxy can replace the blocked page with a customizable web page informing users that the page is blocked. Proxy-based web filtering is the most feature-rich mode, supporting many advanced filters including web content filtering that analyzes web page content according to your custom requirements, Java applet filtering, and blocking invalid URLs.

Flow-based web filtering uses the FortiOS IPS engine to filter web content packets as they pass through the FortiGate unit without any buffering. Flow-based inspection does not use a proxy, so inspected packets are not proxied and altered by the FortiGate unit. Flow-based inspection does not support as many advanced features as proxy-based web filtering.

DNS web filtering employs DNS lookups to the FortiGuard DNS

FEATURES

service to get web page ratings. Filtering is done as part of the DNS lookup and web pages can be blocked or redirected to a web filter block page before the HTTP session starts. As a result, it is lightweight in terms of resource usage although it only supports a limited number of advanced features.

Usage Quota

Administrators can set a daily timed access quota by category or category group. Quotas allow access for a specified length of time or traffic volume, calculated separately for each user.

Safe Search

SafeSearch is a feature of popular search sites that prevents explicit web sites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful user may be able to simply turn it off. Enabling SafeSearch on the FortiGate for the supported search sites can better enforce its use by rewriting the search URL to include the

code to indicate the use of the SafeSearch feature. In addition, FortiOS also provide implementation of YouTube Education Filter.

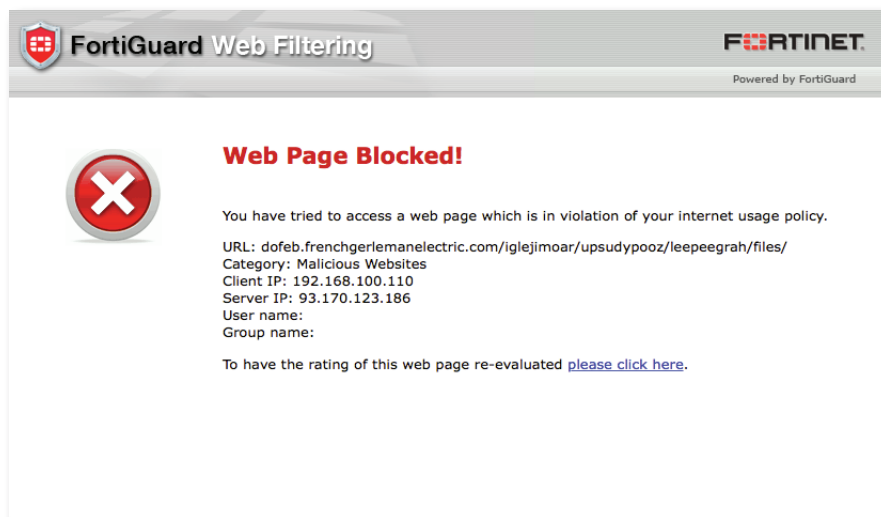
Manual URL and Content Filter

FortiOS web filtering offers specific URL filtering by standard, wildcard, and regular expression definition, as well as content filtering by pattern type and language.

Advanced web filter configurations

FortiOS rich feature set includes ability to implement a number of enterprise features such as:

- Block HTTP redirects by rating, invalid URLs, HTTP POST actions, and Web resume download
- Cookie, Java applet, and ActiveX filter
- Rate Images by URL and URLs by domain and IP address
- Restrict Google account usage to specific domains



FortiGate® - End-to-end Next Generation Firewall

- | | | |
|--|--|--|
| <ul style="list-style-type: none"> ▪ Best Validated protection
FortiGate-based next generation firewall solutions are certified and validated by third-party authorities and programs such as NSS Labs, ICSA, Virus Bulletin, and AV Comparatives for superior security effectiveness. | <ul style="list-style-type: none"> ▪ High Speed and Flexible Connectivity
FortiGate appliances are powered by FortiASICs and designed on purpose-built integrated architecture that provides extremely high throughput and exceptionally low latency. They also offer variety of interfaces for today's network. | <ul style="list-style-type: none"> ▪ Broad Product Offerings
The FortiGate product family scales from desktop units for remote branch offices to high-end platforms for service providers and data centers while virtualized appliances support a wide range of hypervisors and public cloud infrastructure. |
|--|--|--|

FEATURES

Proxy Avoidance Preventions

FortiGate is able to improve the effectiveness of the web filtering by preventing users from evading the security implementation. Organizations can use its multiple integrated technologies including proxy site URL, proxy application control, and IPS proxy behavior blocking.

User and Device Awareness

Most networks in today's organizations are connected with both corporate and personal mobile devices. User and device awareness provides the option to configure intelligent policies that can effectively enforce security.

To tackle the prevalence of BYOD environments, administrators are able to configure web content access policies with sources defined by IPs, users, and devices, either combined or selectively.

External URL Filtering support

In instances where customers have large, existing, deployed implementations of a specific URL filtering solution but replace their

legacy firewalls with a FortiGate family, they can still retain their web filtering infrastructure since FortiOS supports both ICAP and WISP.

Monitoring, Logging, and Reporting

FortiOS empowers an organization to implement security best practices that require continuous monitoring of threats, allowing the organization to adapt to new requirements.

The FortiView dashboards display useful analysis data with detailed and contextual session information, which can be filtered and ranked, with drilldown options also available. This information, including system events activities and administration audit trails, can also be archived via logs.

FortiOS logs all the types of traffic that can connect to or terminate at the FortiGate unit. In turn, these logs can generate useful trending and overview reports.

ADDITIONAL REFERENCE

Resource	URL
FortiOS Handbook - The Complete Guide	http://docs.fortinet.com/fortigate/admin-guides
Fortinet Knowledge Base	http://kb.fortinet.com/
FortiGate Product Page	https://www.fortinet.com/products-services/products/firewall.html



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne 06560
Alpes-Maritimes, France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990